Security analysis of the XYZ protocol

Report for the Computer Security exam at the Politecnico di Torino

Giovanni Pautasso (31415)
tutor: Jack-The-Ripper

September 2018

Contents

```
#include <stdio.h>

int main ()
{
   printf ("Hello!\n");
   return 0;
}
```

Figure 1: An example of a program inserted via `lstlisting`.

```
1 #include <stdio.h>
2
3 int main ()
4 {
5    printf ("Hello!\n");
6    return 0;
7 }
```

Figure 2: Example of a program inserted via `lstlisting` with line numbering.

1 Introduction

Explain here why the XYZ protocol is important and what was the purpose of the present work.

If you want to reference a web site you can do in-line like this – http://www.polito.it – or you can put it in the bibliography when it refers to a project, such as the OpenSSL one [1].

If you want to display source code or program output, you can use the `lstlisting` environment which includes text without altering the original formatting and uses a fixed space font, as in the example in Fig. 1. You can also give numbers to the lines of the program, as in the example in Fig. 2, but numbering should be used only if the text explicitly references specific sections of the program.

To cite short pieces of code you can use directly `lstlisting` in the body text (rather than in a separate figure), as in the following example related to the HTML code for centering a text:

```
<center>
Example of centered text.
</center>
```

2 Protocol description

Describe the protocol in detail, trying to demonstrate knowledge of the topics covered in the course. In other words, don't limit yourself just to list security features but explain why they are important and provide your opinion if they are correctly implemented or could be improved.

You can reference a figure by using the appropriate command, as in the case of Fig. 3, that will be automatically placed on the page and numbered by LaTeX. (NOTE: read the comments in the LaTeX source for this figure as it explains the proper scaling of a figure and the three possible ways to insert it).

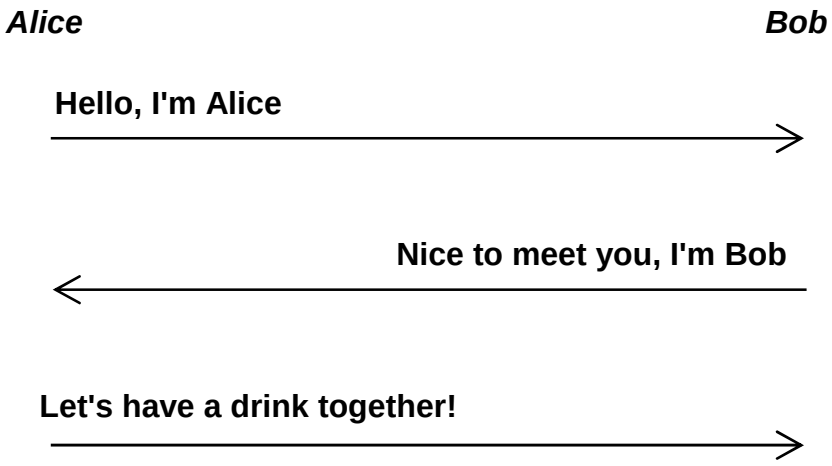

Figure 3: Handshake protocol.

You can also cite papers published at conferences, like [2], or journals [3], an RFC [4], a book [5], or a chapter in a multi-author book [6].

If the section contains a lot of information, you may want to split it into different subsections, each one with a specific focus as done here.

2.1 Request format

The request contains the ID of the caller and the destination IP address, encoded in four different bytes.

On average, it is 10 MB in size. (NOTE: use the siunitx package to properly insert international units when needed, see the LaTeX source for an example on this line and also in Table 1).

2.2 Response format

The response contains a status code (three digits encoded in ASCII) followed by the answer encoded in ISO-8859-1 and terminate with CR LF.

3 Experimental evaluation

Describe:

- general purpose of the experiments (functional evaluation, performance evaluation, comparison with other stuff)
- experimental setup (hardware and software, including detailed build and configuration instructions if needed)

Then describe each experiment: its specific purpose (e.g. testing a specific feature of the protocol), the command run, and the output (expected and actual). You can use a table like Tab. 1 to group the results (for example if the same experiment was repeated with several data sizes)

data size (kB)	*raw transfer time* (ms)	*secure transfer time* (ms)
128	20	22
256	22	30
512	26	37
1024	30	99

Table 1: Experimental results.

For performance testing, remember to run not only experiments with various data size but also – in case of a client-server protocol – stress tests for the server (i.e. increasing number of clients simultaneously requesting attention from the server). Normally the throughput is measured in Mbps.

4 Style

Before delivering your report, don't forget to run a spell checker (MikTeX has an embedded one with a UK-English dictionary).

Remember the difference between open and closed quotes in the normal text and note that LaTeX does them by doubling single quotes "as in this example".

References

[1] The OpenSSL project, http://www.openssl.org/

[2] I. Enrici, M. Ancilli, and A. Lioy, "A psychological approach to information technology security", HSI-2010: 3rd Int. Conf. on Human System Interactions, Rzeszòw (Poland), May 13-15, 2010, pp. 459–466, DOI 10.1109/HSI.2010.5514528

[3] G.Cabiddu, E.Cesena, R.Sassu, D.Vernizzi, G.Ramunno, and A.Lioy, "Trusted Platform Agent", IEEE Software, vol. 28, March-April 2011, pp. 35–41, DOI 10.1109/MS.2010.160

[4] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2." RFC-5246, August 2008, DOI 10.17487/RFC5246

[5] R. J. Anderson, "Security engineering", Wiley, 2008

[6] A.Lioy and G.Ramunno, "Trusted computing", Handbook of Information and Communication Security (P.Stavroulakis and M.Stamp, eds.), pp. 697–717, Springer, 2010, DOI 10.1007/978-3-642-04117-4_32